UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,119	12/31/2003	W. Dale Hopkins	200308859-1	9767

22879 7590 10/04/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
PAIK, STEVE S	
ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 10/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

H·A

Office Action Summary	Application No. 10/750,119	Applicant(s) HOPKINS, W. DALE	
	Examiner Steven S. Paik	Art Unit 2876	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 31 December 2003.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-41 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) 15-41 is/are allowed.

6)☒ Claim(s) 1,10-12 and 14 is/are rejected.

7)☒ Claim(s) 2-9,13 is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 31 December 2003 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 12/31/03.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 10-12 recites the limitation "the host", "the entity-identifier x" and "the entered PIN'" in lines 2 and 4 respectively. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Erfani et al. (US 20030196106 A1) in view of Balph et al. (US 5,631,962).

Re claims 1 and 14, Erfani et al. disclose a smart card that is adapted to partially include and employ a triply-secure algorithm for data exchange. The algorithm verifies a user's identity and his simultaneous membership in any groups that he has joined. The algorithm can be used in smart cards or in computer networks for identity verification and membership proof. A combination of three different hard problems is used. The first one is based on integer factorization, such as the RSA authenticating technique, and the second one is based on a discrete logarithm, and the third one is based on the coefficients of a polynomial function. In a typical application using smart cards, a certification authority (CA) establishes requirements for preparation and issuance of a multi-purpose card.

However, Erfani et al. are silent about a PIN hidden in a polynomial as recited in claim 1.

Balph et al. disclose an electronic key validation process with enhanced security by encrypting the security access codes. A key (an entity-selected PIN) receives data having a hidden polynomial select code and polynomial seed from a host (12). A locally stored (24, 26) select offset and seed offset in the key identifies the location (22) of the select code and seed in the data. The select code decodes (32) into polynomial coefficients which are used to configure a polynomial generator (34). The seed is loaded into the polynomial generator as a starting point of the polynomial (initialization polynomial). The polynomial generator is clocked a number of cycles to calculate a remainder. The select code is modified (28) to select a new polynomial, and the polynomial generator is clocked another number of cycles. The host runs a similar encryption algorithm. The remainder is sent to the host where it is compared with the host generated remainder for key validation. Balph's validation process improves protection of a secret code due to its additional encrypting process.

Therefore, it would have been obvious at the time the invention was made to a person having ordinary skill in the art to have incorporated the encrypting key validation process as taught by Balph et al. into the teachings of Erfani et al. for the purpose of increasing the security of a PIN of a smart card or a computer network system.

Allowable Subject Matter

5. Claims 15-41 are allowable.

6. Claims 2-9 and 13 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter: none of the cited prior art of the record discloses, teaches, or fairly suggests the claimed features comprising, among other things, generating an ephemeral transaction polynomial using a smart card at an entity activated terminal with an entity-entered PIN' enabling recovery from a polynomial over a finite field, the ephemeral transaction polynomial being a function of the entity-entered PIN', the entity-identifier, and a second random number.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

White et al. (US 5,513,263) disclose an access point that utilizes a first password to create an encryption key, then generates a plurality of secondary passwords for use by devices. User device classes are established by assigning a secondary password to a respective class of users, determining the network access permitted the class, determining the network services provided to the class and finally assigning the secondary password to a device seeking to communicate within the network.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Steven S. Paik whose telephone number is 571-272-2404. The examiner can normally be reached on Monday - Friday 5:30a-2:00p (Maxi-Flex*).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on 571-272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Steven S. Paik
Primary Examiner
Art Unit 2876

ssp